clé privée

clé publique

p, q $p \neq q$ premiers

$n = p \cdot q$

n , e

e tel que $\text{pgcd}(e, \varphi(n)) = 1$

Calculer d tel que :

$$ed \equiv 1 \pmod{\varphi(n)}$$

d est la gâche secrète

d, n

chiffrement : $0 \leq m < n$

$$m = c^d \pmod{n}$$

$$c \equiv m^e \pmod{n}$$

Ex 5.4.1

$m = 8$ $\quad p = 7$, $q = 11$, $e = 17$

Annuaire	
Bob	$n = 77$ $\quad e = 17$
Alice	$n = 35$ $\quad e = 7$

Alice $\xrightarrow{\text{Envoi}}$ Bob

$m = 8$ $\qquad\qquad$ $c = 57$

$c \equiv 8^{17} \pmod{77}$ $\qquad$ $17 = 16 + 1$

$8^2 \equiv 64 \pmod{77}$

$8^4 \equiv (8^2)^2 \equiv 15 \pmod{77}$

$8^8 \equiv (8^4)^2 \equiv 71 \pmod{77}$

$8^{16} \equiv (8^8)^2 \equiv 36 \pmod{77}$

$8^{17} \equiv 8 \cdot 8^{16} \equiv 8 \cdot 36 \equiv 57 \pmod{77}$

Calculons d : $\quad ed \equiv 1 \ (\varphi(n))$

$17d \equiv 1 \pmod{60}$ $\qquad$ d est l'inverse de 17 mod 60

$17d + 60k = 1$

$60 = 1 \cdot 60 + 0 \cdot 17$

$17 = 0 \cdot 60 + 1 \cdot 17$

$\vdots$

$1 = 2 \cdot 60 - 7 \cdot 17$

clé secrète
$d = 53$

$d \equiv -7 \equiv 53 \pmod{60}$

$57^{53} \equiv \pmod{77}$ $\qquad$ $53 = 32 + 16 + 4 + 1$

$57^2 \equiv 15 \pmod{77}$

$57^4 \equiv 71 \pmod{77}$

$57^8 \equiv 36 \pmod{77}$

$57^{16} \equiv 64 \pmod{77}$

$57^{32} \equiv 15 \pmod{77}$

$57^{53} \equiv 57 \cdot 71 \cdot 64 \cdot 15 \equiv 8 \pmod{77}$